Updates
June 13, 2019

Regulating the Security of Connected Devices: Are You Ready?

As if businesses did not have enough on their plates as they prepare for the California Consumer Protection Act and similar privacy laws in other states, manufacturers of Internet of Things (IoT) devices (objects that connect to the internet and collect and transmit data) must also comply with California and other states' new IoT device security laws.

While the FTC has previously enforced IoT security under the FTC Act's general prohibition on deceptive and unfair acts and practices, beginning in September 2018, a minor but seemingly growing trend has developed among state legislatures to specifically regulate the security of IoT devices. California SB 327, "Security of Connected Devices" was enacted in September 2018 and will take effect on January 1, 2020. Following California's lead, Illinois, Massachusetts, Maryland, New York, Oregon and Vermont also introduced bills in early 2019 to regulate the security of connected devices. While the Illinois, Maryland and Vermont bills stalled and did not pass during the current legislative session, and the Massachusetts and New York bills have had no movement since they were introduced, the Oregon bill was signed into law on May 30, 2019. These bills, along with the California statute, signal a new era of privacy and security regulation, imposing stringent and often confusing requirements onto IoT device manufacturers.

As companies prepare for the CCPA and other state privacy laws, they should also consider whether this new wave of IoT-related legislation will impact them, and if so, start building a strategy to comply with the California and Oregon IoT laws. These statutes will require companies to take certain security measures to protect the personal information collected and transmitted by connected devices.

Overview of IoT Bills

The California IoT bill imposes security requirements onto manufacturers of IoT devices. The law defines "manufacturers" as persons who manufacture, or contract with another person to manufacture on their behalf, connected devices that are sold or offered for sale in California. Section 1798.91.04(a) of the law requires that manufacturers equip devices with "reasonable security feature(s)" that are (1) "appropriate to the nature and function of the device," (2) "appropriate to the information it may collect, contain, or transmit," and (3) "designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure."

Interestingly, the "reasonable security feature(s)" requirement is automatically satisfied if the device can be authenticated outside of a local area network by a unique, preprogrammed password, or if the device requires a user to generate a new method of authentication (password, biometric identifier or code) before access is granted to the device for the first time. Other than what the statute enumerates, given the broad references to evaluating security for appropriateness based on the nature of the device and the data collected, contained or transmitted by the device, along with the absence of guidance on the meaning of those terms, what constitutes a "reasonable security feature" is somewhat vague. Notably, the statute does not provide for a private right of action; the attorney general, a city attorney, a county counsel or a district attorney have exclusive authority to enforce the law.

The Oregon IoT bill is similar to the California bill in that it requires an IoT device manufacturer to equip the device with reasonable security features. It substantively differs from California's bill, however, in that it only applies to devices "used primarily for personal, family or household purposes." Another substantial difference between the two bills is that a violation of the Oregon law will be considered "an unlawful trade practice" under Oregon's consumer protection law, ORS 646.607, which provides a private right of action. Under Oregon's consumer protection law, the private right of action permits the greater of actual damages or statutory damages of $200, and a court or jury may award punitive damages or equitable relief. Under a class action lawsuit, statutory damages may be awarded only upon a showing of actual loss of money or property.

Potential Issues for IoT Device Manufacturers

Applicability to Existing Devices

It is currently unclear if or how these statutes impact devices already in commerce—the bills do not carve out previously manufactured devices or indicate that the bills only apply to devices manufactured after the effective date. Manufacturers should consider whether existing data security practices and built-in security features could demonstrate "reasonable" security for the devices. Additionally, manufacturers could consider whether compliance is possible through software updates or other off-device security features that can be used to advance the security of the device.

Deference to Federal Law

The California IoT law states that it does not apply to connected devices subject to security requirements under federal law, regulations or guidance promulgated by a federal agency. This may signal that the California legislature is aware of and may even encourage the promulgation of federal privacy and data security bills that cover IoT devices. The Oregon IoT bill also establishes that compliance with "federal law or federal regulations that apply to security measures for connected devices" constitutes a reasonable security feature.

The deference to federal law, however, introduces significant uncertainty around the landscape of what is required. Not only has the FTC, under authority of the FTC Act, established certain requirements regarding IoT device security, in January 2015, the FTC released a Staff Report on the Internet of Things, stating that "what constitutes reasonable security for a given device will depend on a number of factors, including the amount and sensitivity of data collected, the sensitivity of the device's functionality, and the costs of the remedying the security vulnerabilities." While neither bill specifically references FTC enforcement history or other FTC guidance, because the California law defers to federal law, and the Oregon bill establishes that compliance with federal regulations constitutes a "reasonable security feature," the FTC's enforcement history and resulting requirements, and the staff report, may be useful guidance.

Note, however, that what constitutes reasonable security is a shifting standard. While we monitor for updates and developments in this area, IoT device manufacturers would do well to deeply understand and develop a communications strategy regarding their device related security program, the sensitivity of the data collected and the device itself, as well as the scope of work necessary to enhance its security program.

Issues Specific to Industrial IoT Device Manufacturers

While early versions of the California bill suggest it was intended to focus solely on IoT devices in the consumer context, the scope of the final bill is not limited in this way, which means that manufacturers of industrial IoT devices will also need to comply.

The extension of the California law into the industrial IoT space creates some interesting issues and compliance challenges. One such issue is that industrial devices are not necessarily sold directly to the end user. Often, the device is sold to a company or other entity, and the end users are lessees, employees or independent contractors of such company or entity. In this context, the reasonable security features specifically referenced under the law, such as preprogrammed passwords or authentication for each individual user, could be unwieldy or even unnecessary if the information collected through the device cannot be linked back to an identifiable end user.

Recommendations

With the enactment of these new laws, there is now more reason than ever to take steps to secure IoT devices and proactively protect companies, including the following:

- For new products, adhere to secure development lifecycle principals to incorporate security and privacy considerations, compliance requirements and other best practices throughout the entire product development process;
- Begin assessing and documenting the data that IoT devices collect and the sensitivity of that data;
- Document the decision-making process and how the device and its security features work to appropriately secure the device;
- Conduct a security audit and document why the security features are reasonable, and address any security vulnerabilities that are identified; and
- Consider changing product offerings or re-engineering current product offering software to incorporate the required and/or recommended security features.

Authors

Andrew H. Grant

Partner
AGrant@perkinscoie.com 206.359.6376

Explore more in

Privacy & Security Technology Transactions & Privacy Law

Related insights

Update

Securities Enforcement Forum DC 2024: Priorities in the Election’s Wake

Update

The New Administration’s Impact on Retailers